

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-041280

(43)Date of publication of application : 12.02.1999

(51)Int.Cl.

H04L 12/56
H04L 12/22
// G09C 1/00
H04L 9/36

(21)Application number : 09-190302

(71)Applicant : N T T DATA:KK

(22)Date of filing : 15.07.1997

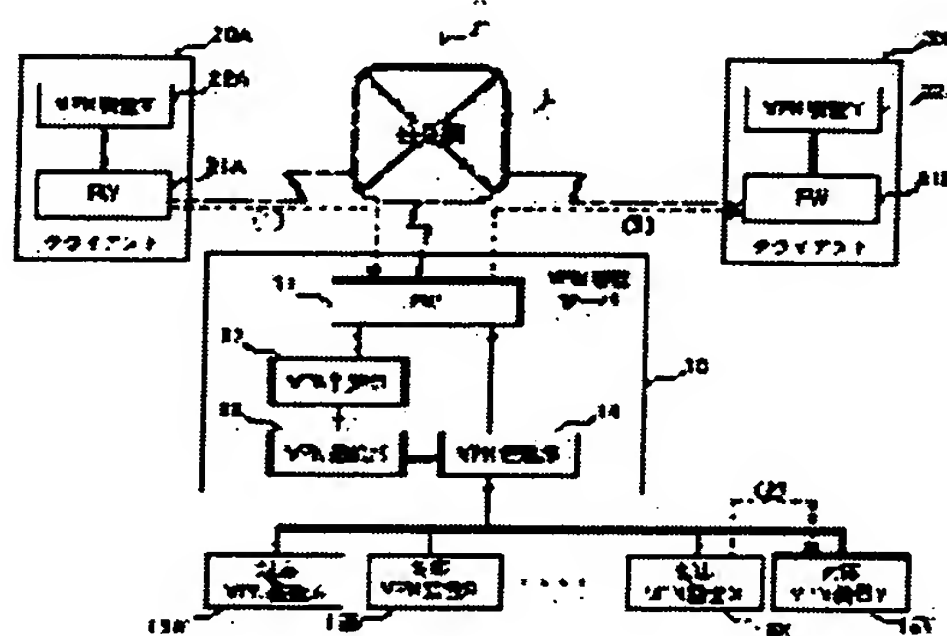
(72)Inventor : MATSUDA YOSHIYUKI
KOBATA YASUHIRO
TSUBOI AKIHISA

(54) COMMUNICATION SYSTEM, VPN REPEATER AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a communication system in which different kinds of virtual private networks(VPN) are compatible.

SOLUTION: A communication system 1 is constituted by providing plural VPN devices 22A and 22B and a VPN managing server 10 equipped with correspondent VPN devices 15X, 15Y... for constructing the VPN on a communication network in cooperation with the respective VPN devices 22A and 22B. The VPN managing server 10 receives an enciphered telegraphic message by constructing the 1st VPN with the VPN device 22A of a telegraphic message transmission source and specifies the VPN device 22B of the transmission destination by deciphering the transmission destination information included in the received enciphered telegraphic message and at the same time, the 2nd VPN is constructed with the VPN device 22B of the transmission source. After the received enciphered telegraphic message is deciphered by a cryptographic key for the 1st VPN, this is enciphered by a cryptographic key for the 2nd VPN and transmitted through the 2nd VPN to the VPN device 22B.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-41280

(43) 公開日 平成11年(1999) 2月12日

(51) IntCl. ⁶	識別記号	F I	
H 0 4 L 12/56		H 0 4 L 11/20	1 0 2 A
12/22		G 0 9 C 1/00	6 6 0 E
// G 0 9 C 1/00	6 6 0	H 0 4 L 11/26	
H 0 4 L 9/36		9/00	6 8 5

審査請求 未請求 請求項の数 6 O L (全 7 頁)

(21) 出願番号 特願平9-190302

(22) 出願日 平成9年(1997) 7月15日

(71) 出願人 000102728

株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目3番3号

(72) 発明者 松田 栄之

東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内

(72) 発明者 木幡 康弘

東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内

(72) 発明者 壺井 彰久

東京都江東区豊洲三丁目3番3号 エヌ・
ティ・ティ・データ通信株式会社内

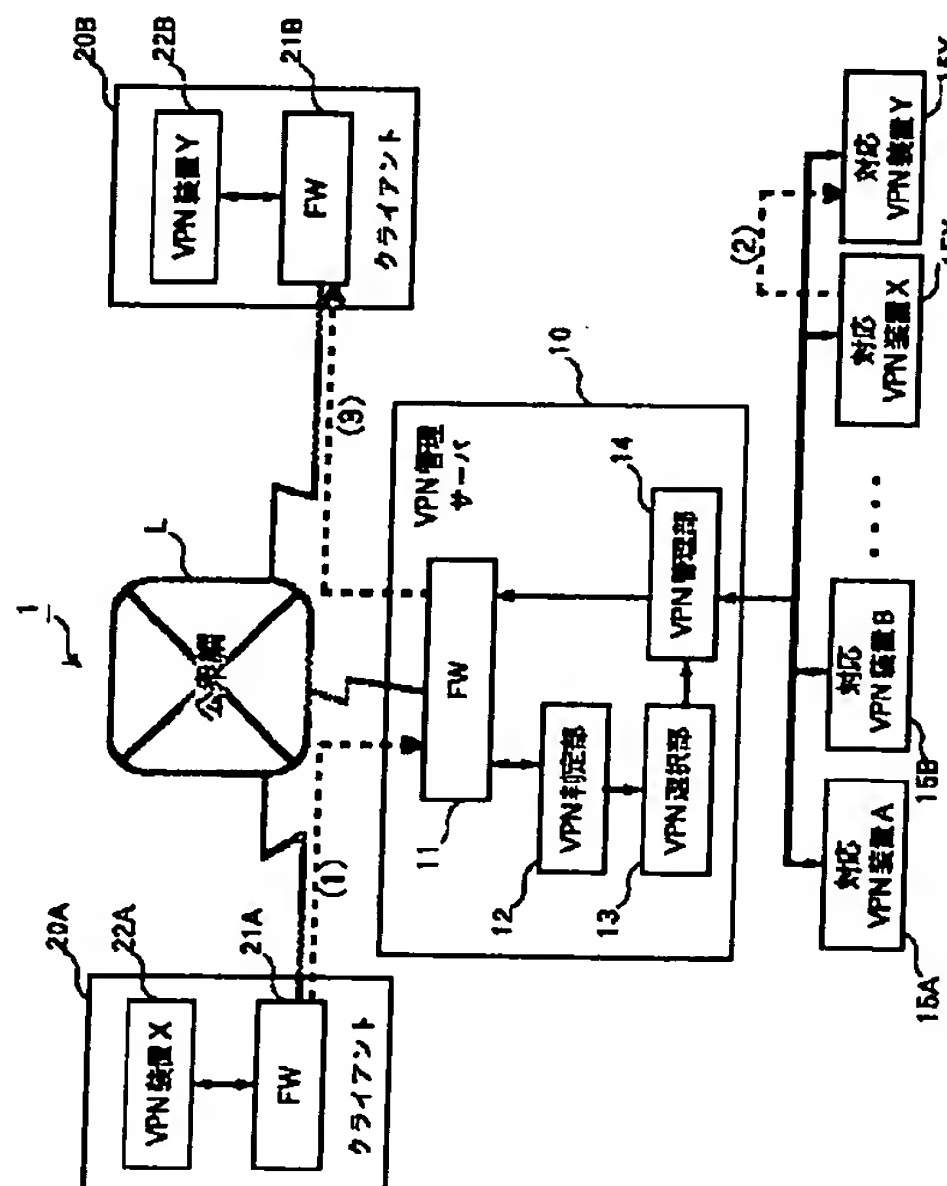
(74) 代理人 弁理士 鈴木 正剛

(54) 【発明の名称】 通信システム、VPN中継装置、記録媒体

(57) 【要約】

【課題】 異種のVPNが互換可能な通信システムを提供する。

【解決手段】 複数のVPN装置22A、22Bと、各VPN装置22A、22Bと協働して通信網上にVPNを構築する対応VPN装置15X、15Y...を具備したVPN管理サーバ10とを含んで通信システム1を構成する。VPN管理サーバ10は、電文送信元のVPN装置22Aとの間に第1VPNを構築して暗号電文を受信し、受信した暗号電文に含まれる送信先情報を解読して送信先のVPN装置22Bを特定するとともに、該送信元のVPN装置22Bとの間に第2VPNを構築する。そして、受信した暗号電文を第1VPN用の暗号鍵で復号化した後、これを第2VPN用の暗号鍵で暗号化し、第2VPNを通じてVPN装置22Bに送信する。



【特許請求の範囲】

【請求項1】 それぞれ同一規格の対応VPN装置との協働により通信網上にVPNを構築する複数のVPN装置と、前記複数のVPN装置に対応するすべての対応VPN装置を具備したVPN中継装置とを含み、

前記VPN中継装置が、

電文送信元のVPN装置との間に第1VPNを構築して暗号電文を受信する手段と、受信した暗号電文に含まれる送信先情報を解読して送信先のVPN装置を特定するとともに、該送信元のVPN装置との間に第2VPNを構築する手段と、前記受信した暗号電文を第2VPN用の暗号電文に変換して第2VPNに送出する手段とを備えて、各VPN装置における電文送信の中継を行うように構成されていることを特徴とする通信システム。

【請求項2】 前記VPN中継装置の前記暗号電文の入出力インタフェース部分にファイアウォールが介在することを特徴とする請求項1記載の通信システム。

【請求項3】 それぞれ同一規格のVPN装置との協働により通信網上にVPNを構築する複数の対応VPN装置と、

電文送信元となる第1VPN装置との間に第1VPN、電文送信先となる第2VPN装置との間に第2VPNを、それぞれ該当する対応VPN装置を用いて構築し、第1VPNを通じて受信した第1VPN装置からの暗号電文を第2VPN用の暗号電文に変換するとともに、変換した暗号電文を第2VPNを通じて第2VPN装置へ送信する経路制御手段と、
を有することを特徴とするVPN中継装置。

【請求項4】 前記複数の対応VPN装置は、それぞれ異なる認証手法、暗号鍵の交換手法、及び暗号化手法に基づいてVPN装置との間にVPNを構築するものであり、前記経路制御手段は、予め用意されたこれらの対応VPN装置から該当する装置を選択して前記第1VPN及び第2VPNを構築することを特徴とする請求項3記載のVPN中継装置。

【請求項5】 前記経路制御手段は、前記第1VPNを通じて受信した暗号電文を前記第1VPN装置の暗号鍵で復号化し、これにより得られた復号電文を前記第2VPN装置の暗号鍵で暗号化して第2VPNへ送出することを特徴とする請求項3または4記載のVPN中継装置。

【請求項6】 それぞれ対応VPN装置との協働により通信網上にVPNを構築するVPN装置に相互通信可能に接続されたコンピュータ装置が読み取り可能なプログラムを記録して成る記録媒体であって、

前記プログラムが、

電文送信元となる第1VPN装置との間に第1VPNを構築して暗号電文を受信する処理、

受信した暗号電文に含まれる送信先情報を解読して送信先の通信装置を特定するとともに、該送信先となる第2

VPN装置との間に第2VPNを構築する処理、及び、前記受信した暗号電文を第2VPN用の暗号電文に変換して第2VPNに送出する処理を前記コンピュータ装置に実行させるものであることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信網上にVPN（Virtual Private Network：仮想専用回線）を構築してデータ通信を行う通信システムに関し、特に、VPNを構築するVPN装置の規格差を吸収する技術に関する。

【0002】

【従来の技術】例えば広域ネットワーク環境を利用した通信システムでは、不正侵入者に対する機密保護等を考慮した高信頼のシステム構築及び運用管理が望まれている。ここに広域ネットワーク環境とは、インターネット等のような広域通信網（ネットワーク）上で送信先経路を制御するルータを介して通信装置相互間のデータ通信を行う環境をいう。ルータは、伝送対象電文の先頭に付加された送信先と送信元のアドレスに基づいて送信先への経路の最適な選択を行う装置である。このようなルータをベースにしたネットワークとしては、企業等の組織内ネットワークや、インターネット・プロバイダのような不特定多数の者に対してネットワーク接続環境を提供するものもあり、その形態は多様化している。また、電話やファクシミリ等に代わる低コストの新たな通信手段として電子メールも定着してきている。このように、今後、電話等の従来回線をネットワーク環境で代替したシステム構築の要求は、急激に増加する傾向にある。

【0003】しかし、広域ネットワーク環境下でのデータ通信では、第三者によるデータ傍受やデータ改竄が容易に起こりうるため、セキュリティ面で問題がある。そのため、例えばエレクトリックコマースの分野で使用される電子通貨のように、機密性の高いデータを通信媒体を用いて伝送しあう場合は、別途、専用回線を敷設する必要があった。そこで、最近では、データ暗号技術、認証技術、対象データを隠蔽するカプセル化技術等を応用し、広域ネットワーク上にVPNを構築してデータ通信を行う技術が提案されている。

【0004】図5は、広域ネットワークである公衆網上にVPNを構築してデータ通信を行う従来の通信システムの一例を示す概念図である。この通信システム2は、データの送受信機能を備えたコンピュータ装置40、50、VPN装置41、51、ファイアウォール（FW）42、52、及びルータ43、53を具備して構成される。FW42、52は、外部からの不正なアクセスに対する保護を特殊なソフトウェアで実現した一種の障壁であり、公衆網Lのような広域ネットワークを使用する環境においては必須なものとなっている。

【0005】通信システム4において、コンピュータ装

置40から遠隔地にある他のコンピュータ装置50に対して電文送信を行う場合の手順は以下になる。まず、送信元及び送信先のルータ43、53間で相互に認証処理を行い、さらに、送信元及び送信先のVPN装置41、51間で、暗号鍵の相互交換を行う。そして、送信元のVPN装置41において、送信先のVPN装置41の暗号鍵を用いて電文を暗号化して送信する。一方、送信先のVPN装置51では、暗号化された電文を受信するとともに、当該電文を送信元のVPN装置51の暗号鍵で復号化してコンピュータ装置50に転送する。

【0006】なお、VPN装置41、51には、他のVPN装置を相互に確認する認証機能、暗号化のための暗号鍵交換機能、電文の暗号化・復号化機能のほか、ルータとしての機能を具備したものもある。これらの機能は、メーカーによる独自方式、或いは標準化方式によって実現されている。また、VPN装置によっては、暗号鍵交換機能を有しないものもあり、必ずしも統一された規格に準拠していないのが現状である。

【0007】

【発明が解決しようとする課題】ところで、VPN装置41、51に具備される認証機能、暗号鍵交換機能、暗号化・復号化等の各機能における規格等の標準化は進められてはいるが、上述のように、現在は、メーカー毎の独自の規格で各機能が実現されて製品化されているため、異なるメーカーの製品間ではVPNを構築することができない。そのため、例えば既にVPN装置を導入している複数の異業種企業が合同のVPNによるネットワーク環境（以下、VPN環境）を構築しようとする場合、同一メーカーの製品を使用すれば問題なくVPN環境が構築可能であるが、異なるメーカーの製品間では、そのままではVPN環境の構築は不可能である。

【0008】そこで本発明の課題は、異種のVPN装置を使用してもVPN環境を構築できる、改良された通信システムを提供することにある。本発明の他の課題は、異種のVPN装置を使用した通信システムにおいて、VPN環境を容易に構築できるVPN中継装置、及びこのVPN中継装置を汎用のコンピュータ装置で実現するための記録媒体を提供することにある。

【0009】

【課題を解決するための手段】上記課題を解決する本発明の通信システムは、それぞれ同一規格の対応VPN装置との協働により通信網上にVPNを構築する複数のVPN装置と、前記複数のVPN装置に対応するすべての対応VPN装置を具備したVPN中継装置とを含み、前記VPN中継装置が、電文送信元のVPN装置との間に第1VPNを構築して暗号電文を受信する手段と、受信した暗号電文に含まれる送信先情報を解読して送信先のVPN装置を特定するとともに、該送信元のVPN装置との間に第2VPNを構築する手段と、前記受信した暗号電文を第2VPN用の暗号電文に変換して第2VPN

に送出する手段とを備えて、各VPN装置間の電文送信の中継を行うように構成されることを特徴とする。

【0010】なお、前記VPN中継装置の前記暗号電文の入出力インタフェース部分には、ファイアウォールが介在するようにする。

【0011】上記他の課題を解決する本発明のVPN中継装置は、それぞれ同一規格のVPN装置との協働により通信網上にVPNを構築する複数の対応VPN装置と、電文送信元となる第1VPN装置との間に第1VPN、電文送信先となる第2VPN装置との間に第2VPNを、それぞれ該当する対応VPN装置を用いて構築し、第1VPNを通じて受信した第1VPN装置からの暗号電文を第2VPN用の暗号電文に変換するとともに、変換した暗号電文を第2VPNを通じて第2VPN装置へ送信する経路制御手段と、を有することを特徴とする。暗号電文の変換は、例えば前記第1VPNを通じて受信した暗号電文を前記第1VPN装置の暗号鍵で復号化し、これにより得られた復号電文を前記第2VPN装置の暗号鍵で暗号化することにより行う。

【0012】なお、前記複数の対応VPN装置は、それぞれ異なる認証手法、暗号鍵の交換手法、及び暗号化手法に基づいてVPN装置との間にVPNを構築するものであり、前記経路制御手段は、予め用意されたこれらの対応VPN装置から該当する装置を選択して前記第1VPN及び第2VPNを構築する。

【0013】上記他の課題を解決する本発明の記録媒体は、それぞれ対応VPN装置との協働により通信網上にVPNを構築するVPN装置に相互通信可能に接続されたコンピュータ装置が読み取り可能なプログラムを記録して成る記録媒体であって、前記プログラムが、下記の処理を当該コンピュータ装置に実行させるものである。

(1) 電文送信元となる第1VPN装置との間に第1VPNを構築して暗号電文を受信する処理、(2) 受信した暗号電文に含まれる送信先情報を解読して送信先の通信装置を特定するとともに、該送信先となる第2VPN装置との間に第2VPNを構築する処理、(3) 前記受信した暗号電文を第2VPN用の暗号電文に変換して第2VPNに送出する処理。

【0014】

【発明の実施の形態】以下、本発明を広域ネットワークによる通信システムに適用した場合の実施の形態を、図面を参照して詳細に説明する。図1は、本実施形態の通信システムの機能ブロック図である。この通信システム1は、電文の送受信を行う複数のクライアント20A、20Bと、本発明のVPN中継装置であるVPN管理サーバ10とを公衆網Lを介して双方向通信可能に接続されて構成される。各クライアント20A、20Bは、FW21A、21B及びVPN装置22A、22Bを具備する通信装置である。

【0015】VPN管理サーバ10は、それぞれ異なる

メーカーにより独自の規格で製品化された複数の対応VPN装置15A, 15B, … 15X, 15Y (以下、特定の対応VPN装置を指す場合以外は、サフィックスを除去した符号15を用いる) が接続された汎用のコンピュータ装置と、このコンピュータ装置に読み取られて実行されたときに、前述のFW11、VPN判定部12、VPN選択部13、及びVPN管理部14の機能を実現するコンピュータプログラムとからなる。このコンピュータプログラムは、通常、コンピュータ装置の内部記憶装置あるいは外部記憶装置に格納され、随時読み取られて実行されるようになっているが、コンピュータ装置とは分離可能な記録媒体、例えばCD-ROMやFD等に格納され、使用時に上記内部記憶装置または外部記憶装置にインストールされて随時実行に供されるものであってもよい。

【0016】なお、本実施形態において、VPN管理サーバ10及び各クライアント20は、各々、既存のルータに相当する通信制御手段を具備しているものとする。また、本実施形態において、各対応VPN装置15は、製品パッケージとして独立に存在し、それぞれ独自の規格によってVPN構築機能を発揮する場合と、VPN管理サーバ10の内部あるいは外部記憶装置に複数且つ異種のVPNソフトウェア (プログラム) を格納しておき、該当するVPNソフトウェアが随時読み出されて実行されることによってVPN構築機能を発揮する場合のいずれであっていてもよい。

【0017】VPN判定部12は、送信元または送信先の各VPN装置22A, 22Bに対応するサーバ側の対応VPN装置15が具備されているかどうかを判定するものである。VPN選択部13は、VPN管理サーバ10が具備している複数の対応VPN装置15から、送信元または送信先のVPN装置22A, 22Bに対応するものを選択するものである。VPN管理部14は、個々の対応VPN装置15の統括制御、認証処理、その他のデータ管理を行うものである。

【0018】次に、本実施形態の通信システム1において、クライアント20A, 20B間で暗号電文の送受を行う場合の処理手順を図2を参照して説明する。この例では、クライアント20AではVPN装置X (22A) を使用し、クライアント20B側では、VPN装置Xと規格が異なるVPN装置Y (22B) を使用するものとする。また、送信対象となる電文に付与されるアドレス情報には、送信先及び送信元のVPN装置X, Y (15X, 22A, 22B, 15Y) によるアドレス情報が使用され、電文に付与される元来のアドレス情報及びデータは、VPN上では暗号化の対象となる。

【0019】いま、クライアント20Aから図3 (a) に示すフォーマットの電文がVPN管理サーバ10に向けて送信されたとする (図1の (1))。VPN管理サーバ10は、FW11を介して受信した電文をVPN判

定部12に送る (ステップS101)。VPN判定部12は、この電文に付与されたアドレス情報から、クライアント20AのVPN装置22Aと協働してVPNを構築するための対応VPN装置がサーバ内に具備されているか否か、つまり、VPN装置Xと対になる対応VPN装置Xが存在するか否かを判定する (ステップS102)。

【0020】対になる対応VPN装置XがVPN管理サーバ10に具備されている場合は、VPN選択部12で、複数のVPN15から該当するものを選択する。この場合の選択方法としては、具体的には、VPN管理サーバ10に具備されている複数のVPN装置15に関する情報を予めVPN選択部12に保持しておき、当該情報と電文に付与されるアドレス情報とを比較し、合致するものを選択するようにする。本例では、VPN装置X (22A) と対になる対応VPN装置X (15X) が存在しているので、これを選択する。この選択情報は、VPN管理部14に入力される。

【0021】VPN管理部14は、選択した対応VPN装置15Xを起動させ、VPN装置22Aとの間にVPNを構築する (ステップS102: Yes, S103)。そして、受信した電文の暗号化部分を、VPN装置15Xの暗号鍵 (VPN装置22Aとの間で交換した暗号鍵) で復号化し (ステップS104)、図3 (b) のようなフォーマットの復号電文を得る。この復号電文から元来の送信先のクライアント20Bを特定するとともに、VPN判定部12でそのクライアントのVPN装置Y (22B) と対になる対応VPN装置YがVPN管理サーバ10に具備されているか否かを判定する (ステップS105)。対になる対応VPN装置YがVPN管理サーバ10に具備されている場合は、VPN選択部12で、該当するものを選択し、VPN管理部14がその対応VPN装置Y (15Y) を起動する (ステップS105: Yes, S106)。そして、対応VPN装置15Yに復号電文を渡して (図1の (2)) これを対応VPN装置の暗号鍵 (VPN装置22Bとの間で交換した暗号鍵) で暗号化し、さらにこの暗号電文に送信先及び送信元のアドレス情報を付与してFW11を介してクライアント20Bに送信する (ステップS107)。このときの電文フォーマットは図3 (c) に示すとおりである。これにより、クライアント20Bは、クライアント20Aからの電文を取得することができる。なお、ステップS102及びステップS105において、対応VPN装置X, YがVPN管理サーバ10に具備されていない場合は、送信元のクライアント20Aにエラー通知を行う (ステップS108)。以上の処理をすべての電文について繰り返す (ステップS109)。

【0022】図4は、本実施形態の通信システム1の概念図である。通常、VPNは、通信を行うクライアント間に直接構築されるが、本実施形態では、図4に示され

るように、複数地点A～Dに存在するクライアントとVPN管理サーバ10との間にそれぞれVPNを構築し、クライアント間の通信は、常にVPN管理サーバ10を経由してこのVPNを通じて行うようにしている。VPN管理サーバ10は、各地点のクライアント側のVPN装置に対応する複数の対応VPN装置を具備しており、各クライアント側のVPN装置間の規格差は、このVPN管理サーバ10で吸収されるので、送信元のクライアントは、送信先のクライアント側のVPN装置の規格を意識することなく、電文を送信することが可能になる。

【0023】このように、本実施形態の通信システム1では、VPN管理サーバ10が、受信した暗号電文を送信元のVPN装置22Aと対になる対応VPN装置15Xで復号化するとともに、復号電文を送信先のVPN装置22Bと対になる対応VPN装置15Yで暗号化してVPN装置22Bに送信するので、異種のVPN装置間の認証機能、暗号鍵交換機能、暗号化・復号化機能等の互換が可能となる。また、対応VPN装置によって異なる暗号鍵を用いた復号化及び暗号化を行うので、機密保護能力の低下も防止することができる。従って、複数地点間において異なるメーカーのVPN装置により構築された異種VPNの使用が可能になり、従来の問題点が解消される。

【0024】なお、本実施形態では、便宜上、クライアント20Aからクライアント20Bへ、異なるVPN装置X、Y(22A、22B)を使用して暗号電文を送信する通信システムの例を説明したが、クライアント20Bからクライアント20Aに暗号電文を送信する場合、あるいは、各クライアント20A、20BのVPN装置が同一規格の場合も同様の手順で電文送信が可能になる。

【0025】

【発明の効果】以上の説明から明らかなように、本発明によれば、VPN管理サーバにおいて、送信元及び送信先のVPN装置との間にVPNが構築する対応VPN装置が選択されて電文送信の中継が行われるので、異種のVPN装置を使用した場合であってもVPN環境の構築が可能となる効果がある。

【図面の簡単な説明】

【図1】本発明の一実施形態に係る通信システムの機能ブロック図。

【図2】VPN管理サーバにおける電文中継の手順説明図。

【図3】(a)は送信元のクライアントからVPN管理サーバに送信される電文のフォーマット、(b)はVPN管理サーバ内で復号された電文のフォーマット、(c)はVPN管理サーバから元来の送信先となるクライアントに送信される電文のフォーマットを示す図。

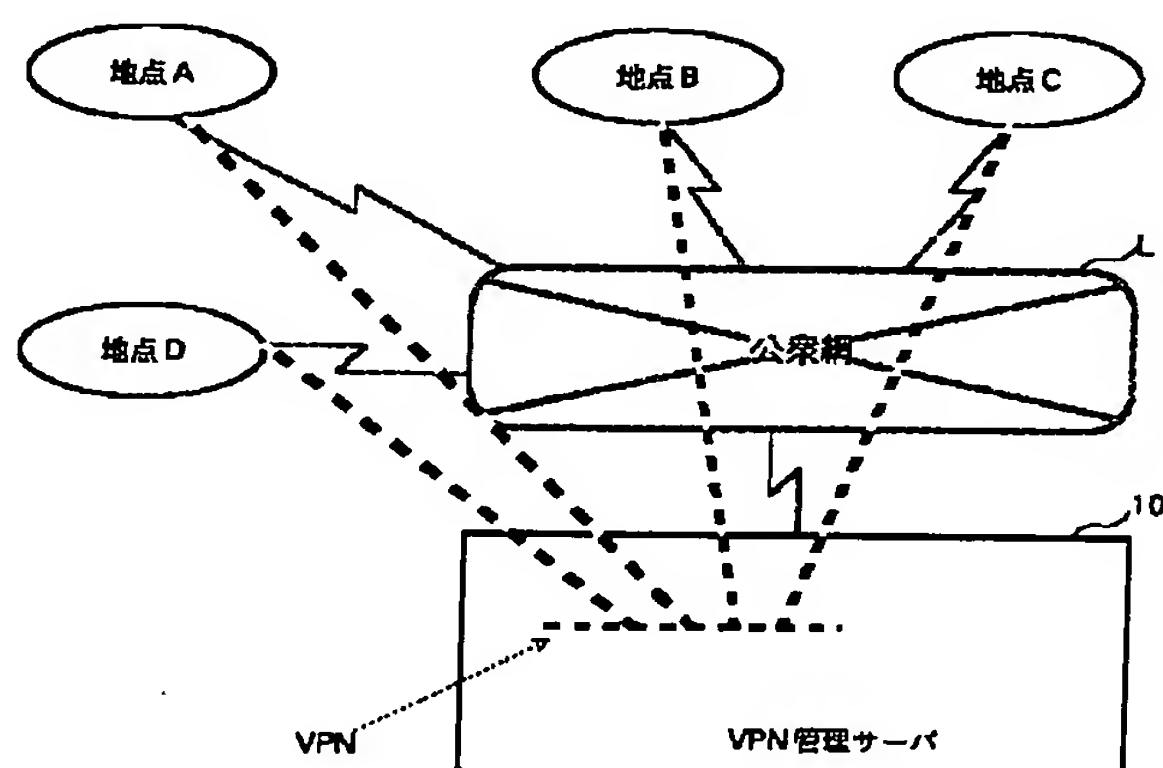
【図4】本実施形態の通信システムにおける動作の概念説明図。

【図5】VPNを使用した従来型の通信システムにおける機能ブロック図。

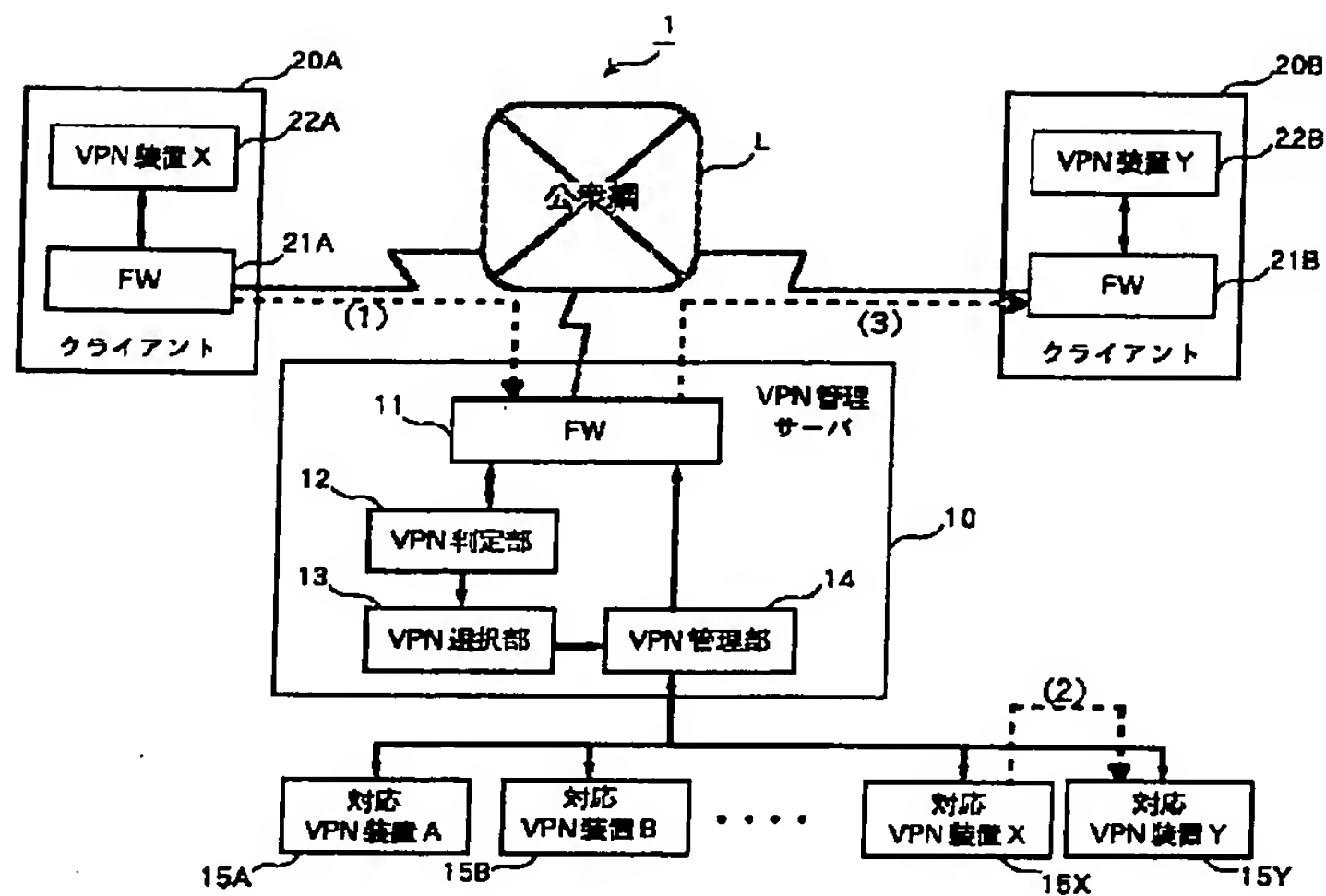
【符号の説明】

- 1 通信システム
- 10 VPN管理サーバ
- 11, 21A, 21B ファイアウォール(FW)
- 12 VPN判定部
- 13 VPN選択部
- 14 VPN管理部
- 15A, 15B, …15X, 15Y 対応VPN装置
- 20A, 20B クライアント
- 22A, 22B VPN装置

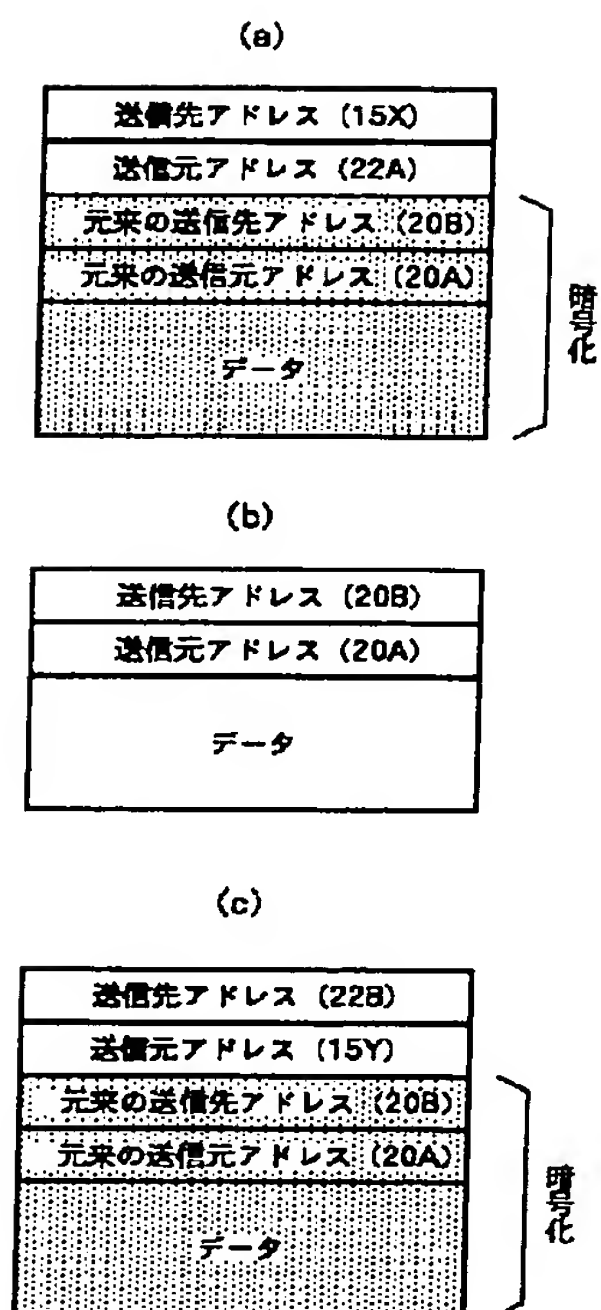
【図4】



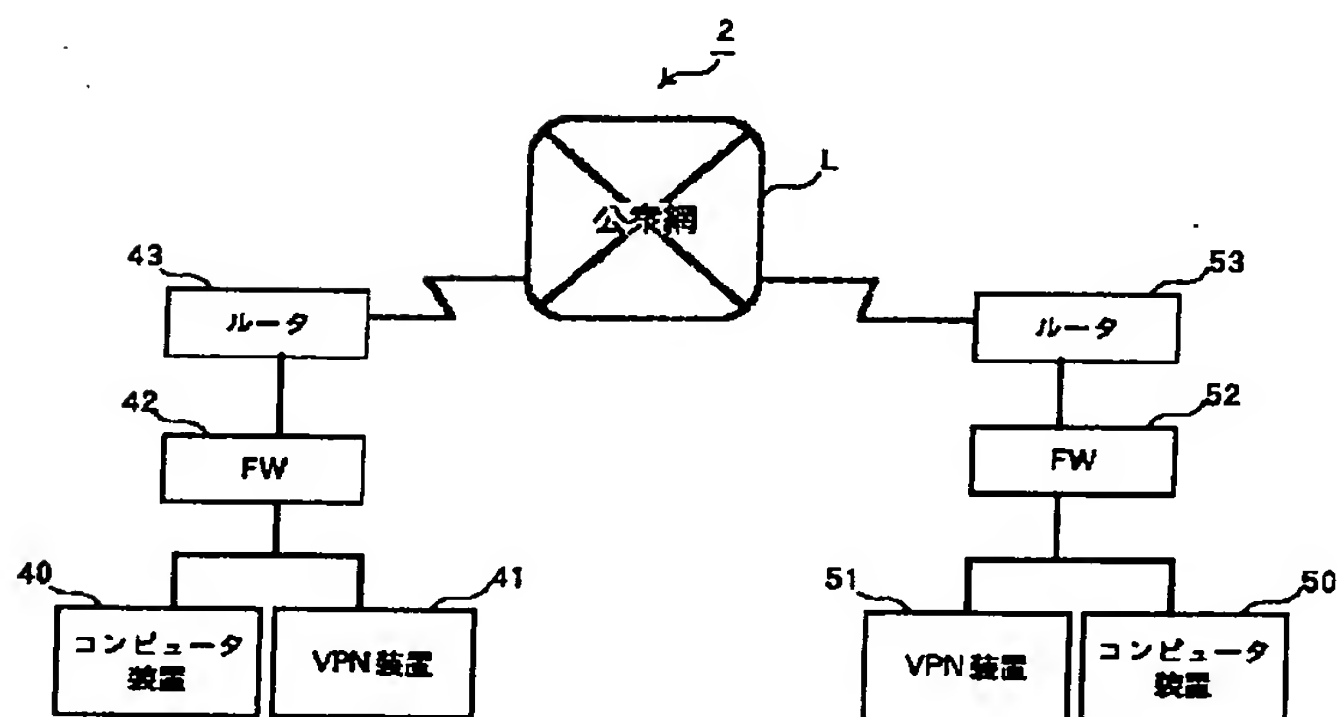
【図1】



【図3】



【図5】



【図2】

